JURISGRADIBUS-*Articles* **ISSN: 2585-3554**

January-March, vol. 1, 2024 Article 3

THE REGULATION OF ARTIFICIAL INTELLIGENCE AND ITS INTEGRATION INTO THE EUROPEAN UNION LAW

Jenifer Ann Shott

DOI:10.5281/zenodo.10963791

Follow this and additional works at:
https://jurisgradibus.free.nf/index.php/jg?i=1

Recommended Citation

Shott, J. A. (2024). The regulation of artificial intelligence and its integration into the European Union law. *Juris Gradibus, January-March, vol. 1,* 82-112, Article 3

Available at:
https://jurisgradibus.free.nf/index.php/jg/issue/view/1

This article is brought to you for free and open access by CEIJ. It has been accepted for inclusion in Juris Gradibus. For more information, please contact: info.jurisgradibus@gmail.com

Doi: 10.5281/zenodo.10963791

THE REGULATION OF ARTIFICIAL INTELLIGENCE AND ITS INTEGRATION INTO THE EUROPEAN UNION LAW

Jenifer Ann Shott, Ph.D, US

Abstract: The time has come to speak for artificial intelligence (AI) after the European regulation proposal. This paper aims to investigate the first impact positive or negative of the AI Act (AIA). The still many problems, the open issues, the points that it has tried to resolve, as well as the control and risk assessment of the artificial intelligence systems, such act, are still points of analysis. The levels of risk, the judgment of the significance of the risk and the evaluation and control of its influence on fundamental rights are additionally points of analysis in this work.

Keywords: AI Act; Artificial intelligence; European Union law; general risk; fundamental rights; valuation risks;

deployers.

INTRODUCTION

In recent years, artificial intelligence (AI) has been a topic of discussion and denial for the existence of human beings both for jurists but also for other sciences. As part of the European Union (EU), intense work began on 21 April 2021 by the European Commission for the adoption of an Artificial Intelligence Act (AIA). A first regulation on the subject for the development, harmonization, production and use of artificial intelligence has been shaped through the European legislator. But in all areas of life the obvious question is: how can artificial intelligence be used? Unfortunately, up until today, even after the adoption of the provisional agreement on 8 December 2023, which arrived after discussions between the Council and the European Parliament, we have no sensational results on the matter but only points of reference and continuous discussion given that problems, gaps but also steps in progress have been presented on the matter[1].

[1] https://www.europarl.europa.eu/news/en/press-room/

Especially, the AIA has the objective of creating a project for the development and use of the AI systems in a precise and extensive way in order to evaluate specific fields and profiles for data protection and, above all, for who is responsible for civil and not only matters. The level of commercialization of new technologies in the European Union adapts to the standards of the AI and its implementations through a logical definition, a European strategy that also influences other regulatory systems and its own standards in ways that are not yet well defined given that they are not always part of legal science.
Coming to hasty conclusions due to the logic used in the AI sector is still very early and the assumptions of AI systems lead to levels of risk. We are referring to levels as they are called: high, limited, minimum and unacceptable. Therefore the European legislator has tried in a proportional way to prevent, mitigate the consequences of the AI with all the possibilities offered by the technology itself and the related application identified such as for example education, justice, essential services that should

20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai.

be used to protect from the one hand certain rights and from the other the daily life. The risks continue to be high, especially the calculation methodology and the related flexible harmonization between member states. Risks also according to the AIA have to do with risk approaches, the meaning of risk, the assessment of the impact on fundamental rights and the risk review procedure. These are systemic risks that have qualified the AI with general objectives, i.e. the General Purpose AI (GPAI) which have also included texts or images (e.g., ChatGpt or Midjourney) as high risk elements. The calculations used for the rating system are not yet finished and the observations of the meaning of risk are applicable to systemic risk in the systems of the GPAI.

Ultimately we can say that a dialogue that carries forward on a political and general agreement in the field of artificial intelligence to arrive at a single text is an open debate between the European Commission, the European Parliament and the Council. The points and powers often overlap, especially with regards to risk analysis and assessment as we see in the next paragraphs.

WHAT ARE THE RISKS FOR THE AIA?

The related risks to protect the activities and the serious consequences of an uncertain nature have as their objective the adoption of necessary precautions to avoid and adopt measures that foresee the risk and harmful effects.

In particular, the risk regulations used are focused on risk management, assessment and communication (Millstone and others, 2004). The AIA has dedicated space to risk management and to the regulatory burdens that are part of the value chain of the AI systems, i.e. deployers and providers. The documents that talk about the logical conception of the AI include political evaluations that the European legislator took into consideration in the AIA. The danger of loss, injury and damage in a general way are consequences of the event, of the activity which for human beings are considered basic and important for the development and future of the AI (Aven, Renn, 2009; Aven, Renn, Rosa, 2011; Florin, Bürkler, 2017).

In practice in the AIA the danger responds to the systems of the AI as the OECD has also described in this regard:

> "(...) machine-based system[s] designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments (...)"[2].

In particular, according to Art. 1 of the AIA the sources of danger are concentrated on an axiological way which responds to the rights and values of the EU of security and democratic procedures[3]. Within this context the AIA includes AI systems in approximately four levels of safety and security risk. A safeguard is found on various entities within the life circle of the AI systems. A risk in such case is, however, not tolerable.

Speaking about the risk of the AIA we are referring to suppliers of the AI systems that require less caution for development. A compliance cost falls to the providers of the risk systems according to Art. 3 (2) of the proposed

[2]OECD Recommendation of the Council on Artificial Intelligence.

[3]Proposal for a Regulation of The European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM/2021/206 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

regulation. Regulatory burdens fall on during the use of the AI systems. Professionals such as managers of large computers, specialized doctors working at hospitals (art. 3 (4)), etc. should meet such burdens. The deployers use a system of instructions for monitoring and respecting the circumstances causing incidents (art. 62) having an impact on data protection (art. 20 (6)).

As regards the administrative sanctions for deployers and providers who try to violate the content of the regulation according to art. 71 of the AIA:

> "(...) in case of non-compliance with the rules on prohibited systems (Article 5), provides for a fine of up to a maximum of 40 million euros; a fine of up to a maximum of 20 million euros for failure to comply with the rules on data management and transparency obligations; a fine of up to 10 million euros for failure to comply with any other requirement or condition (...) the non-compliant is a company which in the previous financial year had an annual worldwide turnover exceeding these figures, then the fine will consist of a percentage of the same; respecting the order, of 7, 4, and 2 percent of the turnover. The concrete measure of the fine must be established considering the nature, severity, and duration

> of non-compliance, but also the size, annual turnover, and any reparative or virtuous conduct of the operator (...). The identification of sanctions of non-monetary nature, which can be associated with or replaced by fines, remains to the Member States, according to principles of effectiveness, proportionality and deterrence. Finally, some administrative sanctions may be imposed by the European Data Protection Supervisor in case of violation of the provisions of the regulation by EU institutions and bodies (...)" (Article 71(6)).

WHICH RULES ARE RISK-BASED?

Reliable standards for the control, design and use of AI systems create an effective type of market that is not yet predefined and as a consequence we do not know how it will function stably in the coming years. A market that should guarantee consumers and their rights as well as be suitable for investors by encouraging and carrying forward technological innovation[4]. The risk of non-approval of a definitive text by 2024 casts doubts on the regulatory

[4] https://www.ncsc.gov.uk/news/uk-develops-new-global-guidelines-ai-security

infrastructure where the EU loses the advantage of the first-mover and must be inclined towards respect for other legal systems that deviate from the logic of the EU. If this were the case, the EU risks losing its way to becoming a cutting-edge market for the evaluation and planning of the development of AI.

Regulating AI means having high levels of protection and safety standards for the production, use and innovation of AI. The risk approach that has been adopted by the EU has various strengths which allows objectives with a precise way to protect the fundamental values of the Union favoring the internal market of the AI. The risk of the AI system compromises values, fundamental rights and the related level of regulation. The risk of the AI system compromises the objectives of governance and makes policy makers accountable for their decisions.

The regulation evaluates the social costs that are connected with AI, also including certification costs that come from malfunctions and violations of all kinds. The AIA as a sort of tax on the negative and high-risk externalities of the AI is focused on deployers and paves the way for evaluating the efficiency of cost and resource allocation.

If the regulations are risk-based, management is also useful, providing answers to terms of a qualitative and quantitative nature of uncertainties that vary according to situations, i.e. epistemic uncertainties (Aven, 2016). Thus, methodologies are provided to prove dangerous events and consequences for the implementation of strategies that prevent and mitigate the related risk.

Evaluating uncertainty means supporting cost-benefits (CBA) in a quantitative way (French, Bedford, Atherton, 2005). Risk management is also based on the acceptance of mitigation costs that exceed the relative benefits given that they are not excessive, thus leading to an intervention that justifies the lower costs, equal to the benefits. Costs are lower when benefits are known (Ale, Hartford, Slater, 2015). These are elements that complement the qualitative assessment that is practiced within the values and fundamental principles of the EU.

The risk that a flexible intervention offers is suitable for political, technological and economic changes according to Articles 84-85.

WHAT ARE THE RISK LIMITS OF THE AIA? WHAT ARE THE RISK LEVELS?

From the previous paragraphs we understood that the AIA in the risk level shows some weaknesses. Weaknesses having to do with the logic of risk, the meaning of risk and the assessment of the impact on fundamental rights[5].

Predetermining risk levels, within the scope of the AIA, do not cause damage to the values of the fundamental rights of the Union as seen from Art. 29A of AIA. These represents the areas of adoption of systems such as work, right of asylum, rule of law, democracy, digitalisation of the EU, etc. (Gonçalves, 2020).

The AIA predetermines the values of the AI system's risk categorization and assessment of the legal values that are involved in specific scenarios. These are strategies that derive from the vision of the dangers of the AI where the dynamics of the sources of danger, vulnerability and risk factors are abandoned (art. 5 (b)), as an evaluation dynamic of the system of the AI. It is an approach that brings the static image of the relevant legal values and fundamental

[5]These are points no. 2 and 3 which were amended from the initial draft and entered into and approved on 14 June 2023.

rights to technical standards of implementation of the precepts which are typically legal (Alexy, 2002).

The risk of negative implications within the scope of the AIA is a static assessment that increases the risk categories that are over- or under-inclusion.

Problems of burdensome legal standards are faced by manufacturers and suppliers when the AI operates in sensitive areas of the AIA. The obligations and guarantees of producers and suppliers to high risk systems are connected with rules that have a cost in terms of internal organization and opportunity costs such as of potential producers, suppliers investing in the European market.

The professional systems adapt a package of obligations that are expected to be high risk where the AI systems automatically organize the training and teaching material. These types of systems have a limiting impact on vulnerable rights of individuals. The malfunctioning of these systems has an impact on the technical interventions that aim to impose on systems an impact assessment on fundamental rights for certification purposes which are certainly required. The risk sector also considers in a significant and possible way the high-level classification of

a consideration system where the assessment of significance is processed at a later time after request according to the methods and time which is certainly often uncertain.

The risk of this type of AI systems can be underestimated. The AI for example that can be used in children's toys should be treated without regulatory burdens. The AI poses risks that reinforce the dependency of engagement techniques and manipulate the behavior of game purchasers.

The AI has a general and successful effect and above all a level of competition as a mover of the EU which gains not only on legal certainty but also on an economic level, thus reducing the European legislative process (Bradford, 2013; Bradford, 2020). Political agreement and risk assessment is an experience that should be followed[6].

Predetermining the level of risk and the advantages in terms of simplicity and uniform procedure in the application of the AIA in a general context facilitates and monitors suppliers and national authorities which makes

[6]https://www.euractiv.com/section/artificial-intelligence/news/eus-ai-act-negotiations-hit-the-brakes-over-foundation-models/.

the procedures simpler, faster and cheaper. This approach meets the adaptation costs in an indirect way for the development and commercialization of the AI systems.
The risk and assessment procedure reveals and provides less certainty that is related to the desired effect. The non-predetermined risk assessment applied to the AIA in a diversified and fragmented way damages the objective of the AIA and the harmonization of the AIA in the Member States of the Union. It is underlined that the guarantee of the AIA uniformly favors a European system where the rules that are susceptible to subjective and arbitrary interpretation lead to the evaluation of the impact of fundamental rights.
These are advantages that predetermine the risk under a simple cost profile that considers the loss of the opportunity cost under risk categories that are efficient in the safety and innovation balance. The assessments burden the procedures and the results which are lighter of the exposed values. In the short term, through the cooperation between institutions of the Union and the national authorities, that supervise this system, the context-specific risk assessment are constant risk factors and identified

within the areas of general application as envisaged in the AIA and in particular in the Annex III.

The uniformity of the AIA follows a discretionary path that emerges through the increase in variables that include risk assessment considering specific situations at a territorial level. Identifying the parameters of the delegated acts and the implementation of the AIA puts the danger of fragmentation at a certainly more specific risk and allows suppliers to classify through a supplementary judgment the significance of the risk (e.g., AIA, Recital 32)[7].

Predetermine the risk of the AIA according to Articles. 84-85 means:

> "(...) (a) introduce a more granular categorization of the risk of AI systems, based on (simulation of) concrete application scenarios; (b) provide for more levels of risk than the four currently envisaged, even in the form of

[7]Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM(2021)0206-C9- 0146/2021-2021/0106(COD): https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html

> sub-levels; (c) further differentiate the regulatory burdens borne by producers, suppliers and users of AI systems, even if they are part of the same risk category (...) substantial changes to the AIA text which, considering the legislative phase in which we find ourselves, are very unlikely (...). They are contained in the significance judgment introduced in the Parliament's compromise text (...) introducing a common methodology to calculate the risk in concrete cases (...)".

Thus, derogations, exceptions, expiry clauses and/or implementation reviews are introduced as similar tools that limit the updating of the relevant list of high risk systems. By facilitating the functioning of the regulatory sandboxes we allow the producers of the AI to experiment the conditions that are requested on a regular basis, such as risk categories which are rigid and also foreseen by the AIA.

WHAT IS THE MEANING OF RISK?

Among the new features of the AIA is the relative judgment of the significance of the risk as was carried out by the European Parliament itself on 14 June 2023:

> "(...) stand-alone AI systems, (...) it is appropriate to

> classify them as high-risk if, in the light of their intended purpose, they pose a significant risk of harm to the health and safety or the fundamental rights of persons and (...) to the environment. Such significant risk of harm should be identified by assessing on the one hand the effect of such risk with respect to its level of severity, intensity, probability of occurrence and duration combined altogether and on the other hand whether the risk can affect an individual, a plurality of persons or a particular group of persons. Such combination could for instance result in a high severity but low probability to affect a natural person, or a high probability to affect a group of persons with a low intensity over a long period of time, depending on the context (...)"[8].

By reading recitals 32, 32A and article 6 (2) together with art. 32 it is understood that:

> "(...) suppliers of high-risk systems can contest and potentially overturn this classification by proving that their AI system, despite operating in the dangerous areas listed in Annex III (e.g., education, employment, health, democratic processes), will not pose real risks to EU legal values, people's fundamental rights or the environment (...) the risk level of its system before launching it on the market the supplier must draw up a summary of the

[8]Recital n. 32 AIA.

> information and the reasons why the system does not represent a significant risk (Recital 32a) and present it to the national supervisory authority (...)".

The supplementary judgment mitigates the predetermination of the risk. This judgment also provides a review criterion that is based on circumstances and a scenario that applies the AI system. Thus the European legislator defined its significance in a generic way and addressed the related problems, namely the judgment of significance and measurement. The recital 32 allows the review of the risk level in a way exclusive to AI systems of a high level. The review criteria of each category promotes measures that are effective and flexible thus making the AI systems appropriate to offer technical solutions to the dangers. The system of the AI classifies at a low level the risk that becomes dangerous highlighting in such a way the significance of the risk and consequently increasing the level of autonomy and other technologies in an extensive way by providing a list of high risk systems for AI that present risks that are comparable, superior, probable to have an impact on fundamental rights according to Art. 7 of the AIA, leaving however ample space for the relative

evaluation in this regard.
This is how we approach the measurement of the significance of risk and how we understand it through recital no. 32. The latter includes some combination elements:

> "(...) the severity, intensity, probability of the occurrence of the event, its duration and, on the other hand, the risk of harming individuals or communities (...). These variables identify some of the most relevant factors in the risk ontology, others of equal importance seem neglected or, when included, considered in isolation (...) on the accuracy of the risk magnitude calculation (...) to evaluate whether and how a categorization system biometric will cause damage, it is not sufficient to estimate the probability of unwanted outcomes based only on the frequency with which certain sources of danger generate damage (...). This probability with other factors, such as the existence of countermeasures is capable of counteracting the occurrence of damage. Thus, for example, risks associated with the origin and management of data cannot be calculated independently of the existence of technical and/or legal safeguards (GDPR) already present and binding. The interaction between all these elements can increase or decrease the

> overall probability of the harmful event and consequently the magnitude of risk (i.e. the probability of the event added to its negative consequences) (...). The implementation of the judgment of significance of the AIA requires the development of a model that considers multiple risk factors and, above all, it places them in a dynamic relationship with each other (...)".

We need an intervention for the next few years on the AIA and any other act on the subject of stabilization of the compliance standards of a general architecture of the regulation. In the implementation documents, the fundamental elements of risk include negative consequences and calculate risk factors in a framework of interactions between them.

Within this context, we note the work of the policy reports of the Intergovernmental Panel on Climate Change (IPCC):

> "(...) the overall risk of a phenomenon must be assessed taking into account not only the sources of danger, the severity of the consequences or the probability, but also of the nature and quantity of the exposed assets, their vulnerability and risk mitigation and prevention strategies (Simpson and others, 2021; Pörtner, and others 2022; Simpson and others, 2023; Ayanlade and others, 2023) (...). The AIA does not ignore these factors, such as

> the vulnerability mentioned in Article 5 (...). It treats them as independent variables with binary realization, which exist or do not exist, and does not consider their interaction as a relevant event for the purposes of the calculation of the significance of the risk (...). The AI risk taxonomy would thus distinguish four main determinants of risk (hazard, exposure, vulnerability, and response), individual components of these determinants (the so-called drivers), and the risk cases external to the observed risk but which influence its magnitude (...)" (Simpson, and others, 2023).

These are factors that include ways of interaction such as:

> "(...) (a) aggregate interactions, whereby risk factors manifest themselves independently, but their combined presence increases the overall risk (...) (b) cumulative interactions, whereby risk factors interact in a specific way, producing a greater impact when combined (...) (c) cascade interaction, whereby one risk factor can trigger others, creating a reaction to chain (...). The AI system leads to risks of unpredictability, ungovernability, violation of copyright and privacy. Risks that emerge as a consequence of characteristics that are not directly linked to each other (...)" (Simpson, and others, 2023).

The risk assessment includes factors such as time which distinguishes the effects in the short and long term by

intensively placing the probability of the risk event and the containment measures (Zio, 2018) as well as those included in resilience i.e. the opposite of vulnerability (Thekdi, Aven, 2023) as elements of an ecological nature of types of risk that make specific use of the AI system and which can influence the regulation itself in an overall way, in other words the ancillary, residual, unpredictable risks and the scarcity of the information collected (Thekdi, Aven, 2023). The concepts specifically and frequently explore the risk assessment of the AI, reiterating the judgment of significance which remains generic in an indistinguishable way at a European level as predetermined elements in the systems of the AI, making the criteria flexible for each type of review.

Intervention in the adopted system of the AIA can also create other problems in risk assessment and related management measures which are only partially managed through non-democratic processing. The European Parliament did not intervene in the technical parameters where the EU provides for democratic representation mechanisms in the implementation acts. By adopting an implementation act, the European Commission, through its

representative committee, follows the comitology process[9]. The committees of the Member States review, evaluate, control for a better way of regulation of the European Commission allowing citizens to provide changes on the executive acts for a better functioning of the AIA (Ballmann, Epstein, O'Happelloran, 2002; Crombez, Huysmans, Van Gestel, 2017).

These mechanisms transfer decision-making power to technical apparatus. In such a way the national supervisory authorities lead to a fragmented application of the AIA and are in contradiction of the very content of the Regulation. The immediate and indirect decision-making power of the Member States is a system that categorizes the regulation towards governance solutions. The AIA together with the rules and the competences of the supranational and national institutions are the coordinators of an implementation system consistent with the messages and principles of the European Parliament. The monitoring and evaluation models are planned through the relevant expert office in the European Commission for future evaluation of

[9] https://commission.europa.eu/law/law-making-process/adopting-eu-law/implementing-and-delegated-acts/comitology_en

the AIA.

The evaluation parameters according to the European legislator also include the AI risk for general purpose (GPAI), i.e. generative models such as the ChatGPT or Bard. High risk systems and the significance of the risk evaluated on a series of factors show the potential work of the computer. The "Floating point Operations Per Second" (FLOPS) presented as a systemic evaluation of control risks based on the hypothesis of a greater power for the calculation of the relevant social models that have a broader nature. This is a partial parameter for reasons that we understood in the previous paragraphs.

WHAT IS THE CONTROL OVER THE FUNDAMENTAL RIGHTS IMPACT ASSESSMENT?

Also on the evaluation of fundamental rights, the European Parliament has included the Fundamental Rights Impact Assessment (FRIA) in the AIA. An evaluation included in Art. 29 (a) of the AIA where deployers of high-risk AI

systems in their work[10] are qualitative compliance standards based on technical reasons by carrying out a first degree assessment identifying prejudices of fundamental rights.

Regarding the scope of the FRIA we are talking about deployers who analyze the use of the AI and the temporal, geographical scope, the impacts on fundamental rights, the consequences of the community that are marginalized and the implications of public governance according to Art. 29A of the AIA. Based on FRIA findings, deployers develop plans that mitigate adverse impacts on fundamental rights by formulating an AI system that informs relevant AI providers at the national level. The evaluation involves the parties who are interested in and the consumer protection and data protection agencies that offer their contributions for a period of six weeks.

The FRIA directly influences the risk classification and includes risk measures for assessing the impact on marginalized groups according to Art. 29, par. f). Thus the

[10] https://www.euractiv.com/section/artificial-intelligence/news/ai-act-eu-countries-mull-options-on-fundamental-rights-sustainability-workplace-use/

FRIA works in a way that resolves the flaws in a static risk model of the AIA when dealing with legal values as well as technical standards leading to outcomes that are predetermined by the values and interests of the community itself.

The impact on fundamental rights is functional to the management of methods. The problems here are also notable and related to the evaluation and impact on the balancing operation. Subjective rights are seen qualitatively as principles that are implemented broadly and without derogating the effectiveness of specific rules of a legal nature (Alexy, 2003). Balancing the rights to complex operations thus pushes deployers to ask expert consultants to outsource this evaluation, thus assuming a cost that is often reasonable for deployers, taking on decisions that are particular and sensitive. A balance without guidelines where the execution of the FRIA coordinates the assessments that the Data Protection Impact Assessments (DPIA) also performs autonomously (Demetzou, 2019).

The FRIA is similar to a form of self-regulation leading to practices that deployers seek to regulate by dedicating

space and time to FRIA assessment and in compliance with fundamental rights protection. This variability in the application of the FRIA causes uncertainties and doubts in the AI industry, thus leaving compliance with the regulatory requirements that accept its products and services on the market and increasing the risk of sanctions at the commercialized level. This situation puts the guarantee and the evaluation of the FRIA in a homogeneous way considering that the deployers follow evaluations of uniform approaches on the weighting of rights involved. Harmonization as a necessity for every regulation is often not just a parliamentary debate which makes the European market less attractive.

These are double track problems that exclude radical solutions and bring the FRIA evaluation into a second line to a model that is not easy and standardized. The choices of a balance between rights and market are rights that use the system of the AI referring to subjective strategies of the deployers ensuring clear and precise methodologies. Thus the list according to Art. 29A of the AIA is continuously transformed and is followed by deployers. The proposals for assessing the impact on fundamental rights are

different from the logic of the European market and the proposals for cooperation and collaboration imply practices that are not yet finished and which require greater commitment from the authorities involved as well as from the managers of the system of the computer practicing AI. These will be the challenges of the next few years in the AI sector.

REFERENCES

Ale, B.J.M., Hartford, D.N.D., Slater, E.D. (2015). ALARP and CBA all in the same game. *Safety Science, 76,* 92ss.

Alexy, R. (2002). *A theory of constitutional rights.* Oxford University Press, Oxford, 2002.

Alexy, R. (2003). On balancing and subsumption. A structural comparison. *Ratio Juris, 16 (4)*, 434ss.

Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research, 253 (1),* 1-13.

Aven, T., Renn, O. (2009). On risk defined as an event where the outcome is uncertain. *Journal of Risk Research 12 (1),* 1-11.

Aven, T., Renn, O., Rosa, E.A. (2011). On the ontological status of the concept of risk. *Safety Science, 49 (8)*, 1075ss.

Ayanlade, A. and others (2023). Complex climate change risk and emerging directions for vulnerability research in Africa. *Climate Risk Management, 40,* 100ss.

Ballmann, A., Epstein, D., O'Halloran, S. (2002). Delegation, comitology, and the separation of powers in the European Union. *International Organization, 56 (3),* 552ss.

Bradford, A. (2013). The Brussels effect. *Northwestern University Law Review, 107 (1),* 5ss.

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press, Oxford.
Crombez, C., Huysmans, M., Van Gestel, W. (2017). Choosing and informative agenda setter. The appointment of the commission in the European Union. *European Union Politics, 18 (2),* 145ss.
Demetzou, K. (2019). Data Protection Impact Assessment: A tool for accountability and the unclarified concept of "high risk" in the General Data Protection Regulation. *Computer Law & Security Review, 35 (6),* 105ss.
Florin, M., Bürkler, M.T. (2017). *Introduction to the IRGC Risk Governance Framework,* Lausanne, EPFL: https://irgc.org/wp-content/uploads/2018/09/IRGC.-2017.-An-introduction-to-the-IRGC-Risk-Governance-Framework.-Revised-version..pdf
French, S., Bedford, T., Atherton, E.E. (2005). Supporting ALARP decision making by cost benefit analysis and multiattribute utility theory. *Journal of Risk Research, 8 (3),* 208ss.
Gonçalves, M.E. (2020). The risk-based approach under the new EU data protection regulation: a critical perspective. *Journal of Risk Research, 23 (2),* 140ss.

Millstone, E. and others. (2004). *Science in trade disputes related to potential risk: Comparative case studies.* European Commission, Spain, 2004.

Pörtner, H., and others (2022). Summary for policymakers. *Climate Change 2022: Impacts, Adaptation and Vulnerability. Contribution of Working Group II to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change,* Cambridge, Cambridge University Press.

Simpson, N. and others (2021). A framework for complex climate change risk assessment. *One Earth, 4 (4),* 492ss.

Simpson, N.P. and others (2023). Adaptation to compound climate risks: A systematic global stocktake. *Science 26 (2).*

Thekdi, S., Aven, E.T. (2023). *Think risk: A practical guide to actively managing risk.* ed. Routledge, London,

Zio, E. (2018). The future of risk assessment. *Reliability Engineering & System Safety, 177,* 178ss.